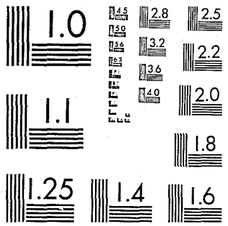

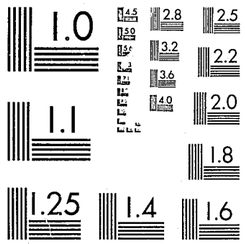

Department of Justice

STATEMENT

OF

ROGER M. OLSEN
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

BEFORE

THE

SUBCOMMITTEE ON CIVIL AND CONSTITUTIONAL RIGHTS
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING

COMPUTER FRAUD

ON

SEPTEMBER 23, 1982

I am pleased to be here today representing the Department of Justice in order to respond to questions concerning the Department's views on computer-related crime. With me representing the FBI are Floyd Clarke, Deputy Assistant Director, Criminal Investigative Division, and William A. Bayse, Assistant Director, Technical Services Division.

All of us are aware of the constant and pervasive impact computers now make on our daily lives. In fact, their use in transactions of every description is so commonplace that even measuring the extent of their use, and the comparable potential for criminal misuse, is very difficult. Nevertheless, in July of this year the Justice Department's Bureau of Justice Statistics published a report entitled Electronic Fund Transfer Systems and Crime. The authors suggested that by 1985 computer terminals either for electronic funds transfer or check verification will be used in at least ten percent of all point of sale transactions such as those in stores and restaurants; that there may be at many as 400 million computer controlled automated teller machine transactions every month; and that the monthly volume of activity in computerized telephone bill-paying accounts could be in excess of $50 million. While these figures represent estimates, they strongly suggest a new vast potential for fraud and other criminal conduct.

The report is also significant for its discussion of the difficulty in defining and measuring the extent of computer crime. For example, in describing the role of computers in electronic funds transfers or EFT's, the report noted that usually traditional legal descriptions of crime--e.g. fraud or theft--can be used to describe EFT crime but such a term reveals little about how the computer was involved in the offense. Moreover, while new classification systems could be developed based on the role of the computer in the crime, the report noted that there is little consensus as to what such classifications should be. Thus, the report's authors decided that "any crime, whether prosecuted or not under traditional or special computer/EFT laws, that would not have occurred but for the presence of an EFT system is considered an EFT crime."[1]

Defining the crime, however, was not of any significant help in measuring its scope. The report noted that there is no single source of data about computer or EFT crime and described four studies which were identified as those most likely to provide reliable information on the nature and extent of EFT crime. A review of these and other sources led to the conclusion that there is no "valid data for measuring and understanding the nature and extent of EFT crime."[2]

1/ Computer Crime, Electronic Fund Transfer Systems and Crime, July 1982, Executive Summary, p. vii. (Hereafter Computer Crime.)

2/ Computer Crime, Executive Summary, pp. xi-xii.

Nevertheless, the sheer magnitude and dollar volume of the transactions handled by computers has caused significant discussion in the law enforcement community and in the data processing industry about computer security and the use or abuse of computers to perpetrate crime. The Congress has also expressed an interest in devising a statute designed to safeguard the integrity of computer operations. A bill to accomplish this, S., 240 was introduced by former Senator Ribicoff in the 96th Congress. The Department of Justice took an active role in helping to make this statute effective from the criminal prosecutor's standpoint.

At present, as you are aware, there is no sanction available specifically dealing with computer-related crime. Any enforcement action in response to criminal conduct indirectly or directly related to computers must rely upon a statutory restriction dealing with some other offense. This requires the law enforcement officer, initially the agent, and then the prosecutor, to attempt to create a "theory of prosecution" which somehow fits what may be the square peg of computer fraud into the round hole of theft, embezzlement or even the illegal conversion of trade secrets. The crafting of such a theory can be awkward, and the results far from perfect. Even if a theory is devised which apparently covers the illegal acts, it still must be treated as an untested, untried basis of prosecution in the trial court. This can lead to the dismissal of a

prosecution, notwithstanding the egregious nature of the crime or the extensiveness of trial preparation, because decades old statutory elements designed to deal with other crimes have been stretched too far to accommodate modern criminality. The potential magnitude of the harm that could be done by misuse of a computer suggests that there is merit in legislation that would directly address computer crime, and the power to regulate commerce and the power of the federal government to punish crimes where the government is itself the victim would provide a constitutional basis for such a statute.

A limited approach would be to reach computer crime involving federal government-owned computers, and those of financial institutions insured by the United States; if a broader approach were to be favored, the statute could be expanded to reach computers operating in or affecting interstate commerce. The types of conduct that would be proscribed would include: (1) fraud in the use of a computer (where the computer is the vehicle much as the mails and wire communication are the vehicles in the mail and wire fraud statutes); (2) theft of property, services or money through the use of or in the illegal access to these computers; and (3) the illegal use, damage or destruction of such computers.

In our rendering assistance in the drafting of the Ribicoff bill to address these activities, classical fraud language was incorporated in order to suggest reliance on existing legal

interpretations of mail and wire fraud cases. This was done to assure that the computer fraud statute would have solid legal underpinnings in serving to cover virtually any type of bogus scheme using the designated computers. Further, an illegal access, damage, and destruction clause was incorporated because of the unusual nature and remarkable quantity and quality of harm a single unauthorized access or destructive act can wreak when a significant computer or system is the target.

As I indicated previously, statistics detailing the extent of computer crime are simply not available and consequently, I cannot, in all candor, represent that legislation in this area is clearly needed. Notwithstanding, the experience of law enforcement in the various instances of computer-related crime that have by their size or nature drawn notice, suggests that we may fail ourselves by not being forearmed with an appropriately drafted statute. Two well known examples present themselves. The Seidlitz case, tried in the District of Maryland, and the Rivkin case in the California state court system are examples of computer-related crime which, if perpetrated in a slightly different manner, might well have escaped even the possibility of federal prosecution.

In Seidlitz, the owner of a computer company stole confidential software by tapping into the computer system of a previous employer from his own remote terminal. Had the defendant not made two of the fifty access calls across state

lines, there would have been no basis for federal prosecution; only a statute on theft of trade secrets would have remained as as possible recourse.

In Rivkin, a computer expert fradulently used a bank's in-house access codes to transfer millions of dollars to accounts he controlled in another bank. If federal jurisdiction had been sought and the wire communication transferring the funds had all been within the same state, we would have been hard-pressed to prosecute.

Such instances in which the use of interstate facilities is avoided by the perpetrator would leave federal law enforcement without an appropriate weapon and effectively foreclosed from addressing what might be properly perceived as an area of significant federal interest. With that in mind, I would like to invite the committee's attention to Mr. Clarke and Mr. Bayse of the FBI who will address this matter from the investigative perspective. Thereafter I will be please to respond to questions.

END